Avis du Contrôleur européen de la protection des données

sur la communication conjointe de la Commission et de la haute représentante de l'Union européenne pour les affaires étrangères et la politique de sécurité intitulée «Stratégie de cybersécurité de l'Union européenne: un cyberespace ouvert, sûr et sécurisé» et sur la proposition de directive de la Commission concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans l'Union

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 16,

vu la Charte des droits fondamentaux de l'Union européenne, et notamment ses articles 7 et 8,

vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[1],

vu le règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données[2], et notamment son article 28, paragraphe 2,

A ADOPTÉ L'AVIS SUIVANT:

1. INTRODUCTION

1.1. Consultation du CEPD

1. Le 7 février 2013, la Commission et la haute représentante de l'Union européenne pour les affaires étrangères et la politique de sécurité ont adopté une communication conjointe au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions intitulée «Stratégie de cybersécurité de l'Union européenne: un cyberespace ouvert, sûr et sécurisé»[3] (ci-après la «communication conjointe», la «stratégie de cybersécurité» ou la «stratégie»).

2. Le même jour, la Commission a adopté une proposition de directive du Parlement européen et du Conseil concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information dans

[1] JO L 281 du 23.11.1995, p. 31.
[2] JO L 8 du 12.1.2001, p. 1.
[3] JOIN (2013) 1 final.

Adresse postale: rue Wiertz 60 - B-1047 Bruxelles
Bureaux: rue Montoyer 30
Courriel: edps@edps.europa.eu – Site web: www.edps.europa.eu
Tél.: 02-283 19 00 - Fax: 02-283 19 50

l'Union[4] (ci-après la «directive proposée» ou la «proposition»). Cette proposition a été transmise au CEPD à des fins de consultation le 7 février 2013.

3. Avant l'adoption de la communication conjointe et de la proposition, le CEPD a eu la possibilité de formuler des commentaires non officiels à la Commission. Il se félicite que certains de ses commentaires aient été pris en considération dans la communication conjointe et dans la proposition.

1.2. Objectifs de la stratégie de cybersécurité et de la directive proposée

4. La communication conjointe établit la stratégie de cybersécurité de l'Union et expose la vision globale de l'Union européenne en ce qui concerne les meilleurs moyens de prévenir les perturbations et attaques visant le cyberespace et de s'y opposer[5]. Elle définit cinq priorités et actions stratégiques:

   - parvenir à la cyber-résilience[6];
   - faire reculer considérablement la cybercriminalité[7];
   - développer une politique et des moyens de cyberdéfense en liaison avec la politique de sécurité et de défense commune (PSDC)[8];
   - développer les ressources industrielles et technologiques en matière de cybersécurité;
   - instaurer une politique internationale de l'Union européenne cohérente en matière de cyberespace et promouvoir les valeurs essentielles de l'Union.

5. La section 1.2 de la communication conjointe dispose que les actions recensées dans la stratégie de cybersécurité seront guidées par le respect des valeurs essentielles de l'Union et par la protection des libertés et droits fondamentaux consacrés par la Charte des droits fondamentaux de l'Union européenne, notamment des données à caractère personnel et du respect de la vie privée.

---

[4] COM (2013) 48 final.

[5] Voir le communiqué de presse de la Commission européenne et du Service européen pour l'action extérieure IP/13/94, 7 février 2013.

[6] Le concept de «cyber-résilience» n'est défini ni dans la communication conjointe, ni dans la directive proposée sur la sécurité des réseaux et de l'information. Il peut toutefois être compris au sens de sécurité telle que définie dans la directive proposée, peut-être avec l'élément supplémentaire de la faculté d'un système à se remettre des effets d'un incident de sécurité jusqu'à retrouver sa pleine capacité opérationnelle. Le manque de clarté de ce terme central de la communication est regrettable et constitue une faiblesse importante de la stratégie.

[7] La «cybercriminalité» est définie à la note de bas de page 5 de la communication conjointe comme étant «*un large éventail d'activités criminelles dont les ordinateurs et systèmes informatiques constituent soit l'arme soit la cible principale. La cybercriminalité recouvre les délits habituels (fraude, contrefaçon et usurpation d'identité p. ex.), les délits liés au contenu (distribution en ligne de matériel pédopornographique ou incitation à la haine raciale p. ex.) et les délits spécifiques aux ordinateurs et systèmes informatiques (attaque contre un système informatique, déni de service et logiciel malveillant p. ex.).*»

[8] La communication conjointe ne donne aucune définition de la «cyberdéfense». Les actions envisagées dans ce domaine visent à accroître la résilience des systèmes de communication et d'information préservant les intérêts des États membres en matière de défense et de sécurité nationale.

6. La communication conjointe présente un calendrier commun pour que les États membres, la Commission, le Parlement européen, le Conseil, l'ENISA, Europol et l'industrie œuvrent ensemble à la réalisation des objectifs de la stratégie. Elle propose de réunir toutes les parties prenantes dans le cadre d'une conférence de haut niveau et de mesurer les progrès accomplis dans 12 mois.

7. La directive proposée est présentée comme étant l'une des principales mesures qui contribueront à mettre en œuvre l'action 1 de la stratégie de cybersécurité, dont le but est d'aider à «parvenir à la cyber-résilience». La proposition a pour objectif d'assurer un niveau élevé commun de sécurité des réseaux et de l'information (SRI) au sein de l'Union européenne. En particulier, la proposition prévoit:

   - des obligations aux États membres en ce qui concerne la prévention et la gestion des risques et incidents touchant les réseaux et systèmes informatiques ainsi que les interventions en cas d'événement de ce type;
   - la création d'un mécanisme de coopération entre les États membres et la Commission, afin de partager, de façon coordonnée et efficace dans le cadre d'une infrastructure sécurisée, des alertes rapides sur les risques et incidents, ainsi qu'afin de coopérer et d'organiser régulièrement des examens par les pairs; et
   - l'obligation, pour les acteurs du marché et les administrations publiques, d'adopter des pratiques en matière de gestion des risques et de communiquer les incidents qui ont un impact significatif sur la sécurité des services essentiels qu'ils fournissent.

1.3. Pertinence de la protection des données pour le paquet cybersécurité et objectif de l'avis du CEPD

8. Le CEPD se félicite que l'Union européenne ait présenté une stratégie globale visant une sécurité accrue sur l'internet[9], complétée par la proposition de directive concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information (SRI) à travers l'Union. Plusieurs régions dans le monde ont adopté ou sont en train d'adopter des stratégies de cybersécurité afin de répondre aux risques et aux menaces qui apparaissent sur l'internet. Il était devenu essentiel que l'Union adopte sa propre stratégie pour aborder ces questions d'une façon qui tienne également compte de la dimension internationale des défis pour la sécurité qui sont rencontrés dans le cyberespace.

9. La stratégie de cybersécurité s'inscrit dans la continuité de la politique qui a été élaborée par l'Union dans le domaine de la sécurité des réseaux et de l'information (SRI): en 2001, la Commission a publié une communication

[9] L'absence de stratégie globale de sécurité intérieure de l'Union avait notamment été soulevée dans l'avis du CEPD sur la communication de la Commission au Parlement européen et au Conseil – «La stratégie de sécurité intérieure de l'UE en action: cinq étapes vers une Europe plus sûre», publié le 17 décembre 2010, JO C 101/6.

intitulée «Sécurité des réseaux et de l'information: Proposition pour une approche politique européenne»[10] et, en 2006, elle a publié une stratégie pour une société de l'information sûre[11]. Pendant de nombreuses années, la politique de l'Union dans le domaine de la SRI s'est principalement centrée sur la sécurité. Dans ce contexte, les droits au respect de la vie privée et à la protection des données ont longtemps été considérés comme opposés à l'objectif de la sécurité («sécurité contre respect de la vie privée») et, jusqu'à présent, ils n'ont donc été abordés que marginalement dans le cadre de la politique de l'UE en matière de SRI. De ce point de vue, le CEPD salue la reconnaissance explicite du respect de la vie privée et de la protection des données dans la stratégie, ainsi que le fait que celles-ci soient considérées comme des valeurs essentielles qui devraient guider la politique de cybersécurité dans l'Union et au niveau international[12].

10. En raison de l'utilisation sans cesse croissante des technologies de l'information et des communications (TIC), le CEPD estime que des mesures destinées à assurer un niveau élevé de sécurité sur l'internet devraient contribuer à améliorer la sécurité de toutes les informations qui y sont traitées, y compris les données à caractère personnel. Le CEPD souligne que la sécurité du traitement des données a toujours constitué un élément crucial de la protection des données[13]. Dans ce contexte, l'adoption par l'Union de la stratégie de cybersécurité et de la directive proposée sur un niveau élevé commun de SRI peut jouer un rôle fondamental en contribuant à garantir la protection des droits des personnes au respect de la vie privée et à la protection des données dans l'environnement en ligne[14].

11. Par ailleurs, le CEPD souligne que la poursuite de l'objectif de cybersécurité peut conduire à la mise en place de mesures qui portent atteinte aux droits de la personne au respect de la vie privée et à la protection de ses données à caractère personnel, tels que définis dans la Convention européenne des droits de l'homme, dans le traité sur le fonctionnement de l'Union européenne et dans la Charte des droits fondamentaux de l'Union européenne[15]. Le CEPD rappelle que toute atteinte aux droits fondamentaux de la personne ou toute limitation de ces droits doit respecter l'article 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne. Étant donné qu'un nombre croissant de données à caractère personnel font l'objet d'un traitement par les systèmes et les réseaux informatiques, il convient de s'assurer qu'aucune mesure appliquée dans le cadre de la stratégie de cybersécurité visant à contrôler et améliorer la sécurité des systèmes et réseaux informatiques ne

[10] COM(2001)298.
[11] COM(2006)251.
[12] Voir la section 1.2., page 3.
[13] Des exigences en matière de sécurité sont prévues aux articles 22 et 35 du règlement (CE) n° 45/2001, aux articles 16 et 17 de la directive 95/46/CE et aux articles 4 et 5 de la directive 2002/58/CE, ainsi qu'à l'article 7 de la convention sur la protection des données, adoptée en 1981 dans le contexte du Conseil de l'Europe et désormais ratifiée par tous les États membres de l'UE.
[14] Voir également le discours de M[me] Viviane Reding, vice-présidente de la Commission européenne, «The EU's data protection rules and the Cyber Security Strategy: two sides of the same coin», 19 mai 2013, disponible à l'adresse: http://europa.eu/rapid/press-release_SPEECH-13-436_en.htm?locale=en
[15] Voir l'article 8 de la CEDH, l'article 16 du TFUE et les articles 7 et 8 de la Charte.

s'immisce dans la vie privée des personnes de façon disproportionnée, notamment en accédant indûment à leurs données à caractère personnel.

12. Par conséquent, le CEPD souligne qu'il importe que tous les droits fondamentaux soient dûment pris en considération dans la stratégie de cybersécurité et dans toutes ses actions de mise en œuvre, notamment, d'une part, la protection des personnes contre les menaces à la cybersécurité et d'autre part, la protection de leur vie privée et du droit à la protection de leurs données à caractère personnel. Le CEPD insiste sur le fait que toute politique mise en œuvre au sein de l'Union en matière de cybersécurité, et toute mesure prise dans ce cadre, doit être élaborée avec précaution, de manière à éviter toute atteinte illégale aux droits de la personne au respect de sa vie privée et à la protection de ses données, notamment en veillant à ce qu'elle respecte les principes de nécessité et de proportionnalité, ainsi que la législation applicable en matière de protection des données.

13. Le CEPD prend note de ce que l'exposé des motifs de la directive proposée reconnaît, à sa section 1.3, que tous les acteurs qui sont responsables du traitement de données sont obligés par le cadre réglementaire en matière de protection des données d'instaurer des mesures de sécurité destinées à protéger les données à caractère personnel, et que cette obligation est en train d'être renforcée par la réforme en cours du cadre relatif à la protection des données, y compris par une obligation de notification des violations. La stratégie de cybersécurité reconnaît aussi, à sa section 2.1, que la législation sur la protection des données actuellement en vigueur exige des responsables du traitement des données qu'ils prévoient des exigences de protection et des mesures de sauvegarde des données, y compris des mesures relatives à la sécurité. Étant donné qu'une part considérable de toutes les activités des réseaux et systèmes informatiques visées dans la stratégie et dans la directive proposée porteront sur le traitement de données à caractère personnel, l'obligation prévue dans la législation relative à la protection des données est probablement l'obligation la plus globale en matière de sécurité des réseaux et de l'information qui existe dans le cadre du droit de l'Union. Il convient également de noter que les principes à respecter lors de l'élaboration de mesures de sécurité d'ordre technique et organisationnel adaptées, sur la base d'une évaluation et d'une gestion des risques et compte tenu de l'état le plus avancé de la technique et du coût de chaque mesure, présentés dans la directive proposée sont les mêmes que ceux déjà définis dans la législation relative à la protection des données.

14. Il est toutefois regrettable que la stratégie de cybersécurité et la directive proposée ne soulignent pas davantage la contribution à la sécurité de la législation existante et à venir en matière de protection des données, qu'elles ne garantissent pas pleinement que toutes les obligations découlant de la directive proposée ou d'autres éléments de la stratégie soient complémentaires aux obligations de protection des données et que les unes et les autres ne se chevauchent pas ni ne se contredisent. Le rôle majeur joué par les autorités chargées de la protection des données dans la mise en œuvre et l'exécution de ces obligations n'est pas non plus dûment pris en considération. Ces aspects seront examinés plus avant aux chapitres 2 et 3 ci-dessous relatifs, d'une part,

à la stratégie de cybersécurité de l'UE et, d'autre part, à la directive proposée sur la sécurité des réseaux et de l'information.

2. ANALYSE DE LA STRATÉGIE DE CYBERSÉCURITÉ DE L'UNION

2.1. Commentaires généraux sur la stratégie de cybersécurité de l'Union

15. Le CEPD constate que la proposition de règlement général sur la protection des données[16] n'a pas été prise en considération dans la stratégie de cybersécurité. Par ailleurs, il n'a pas non plus été tenu compte de l'initiative en cours en vue d'un règlement sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur[17] dans la stratégie de cybersécurité. Il n'y est fait référence qu'indirectement dans la directive proposée qui exclut de son champ d'application les fournisseurs de services de confiance. Il est regrettable que lors de la préparation de la stratégie de cybersécurité[18], le rôle des services de confiance et des services d'identification électronique sécurisée n'ait pas été dûment analysé.

16. En raison de l'absence d'un examen soigneux et d'une prise en considération rigoureuse d'autres initiatives parallèles de la Commission et des procédures législatives en cours, comme la réforme de la protection des données et le règlement proposé sur l'identification électronique et les services de confiance, la stratégie de cybersécurité n'offre pas de vision véritablement complète et globale de la cybersécurité au sein de l'Union et risque de perpétuer une approche fragmentée et compartimentée.

17. La communication conjointe insiste sur plusieurs principes, y compris les droits au respect de la vie privée et à la protection des données, lesquels devraient inspirer la politique de cybersécurité dans l'UE et au niveau international. Elle reconnaît qu'au niveau international, l'Union a un rôle à jouer en promouvant la liberté et en veillant au respect des droits fondamentaux en ligne[19]. Le CEPD accueille positivement le fait que la protection des droits fondamentaux à la protection de la vie privée et des données ait été explicitement mentionnée parmi les principes qui doivent guider la stratégie de cybersécurité.

18. Le CEPD constate aussi avec satisfaction que des références explicites aux obligations de protection de la vie privée et des données ont été incluses dans plusieurs actions de la stratégie. Par exemple:
    - la communication conjointe prévoit explicitement, en page 4, que «Tout partage d'informations à des fins de cybersécurité, dès lors que

[16] COM (2012) 11 final.
[17] COM (2012) 238 final.
[18] Les questions de protection des données soulevées dans ce contexte sont mises en évidence dans l'avis du CEPD du 27 septembre 2012 sur la proposition de la Commission relative à un règlement du Parlement européen et du Conseil sur la confiance pour les transactions électroniques au sein du marché intérieur (règlement sur les services de confiance électroniques), disponible à la section Consultation du site web du CEPD, à l'adresse: www.edps.europa.eu.
[19] Voir la communication conjointe, p. 3.

des données à caractère personnel sont en jeu, doit être conforme au droit de l'UE en matière de protection des données et tenir dûment compte des droits des personnes dans ce domaine»;
- la note de bas de page 7, en page 5, indique que les actions de la stratégie relatives au partage d'informations, dès lors que des données à caractère personnel sont en jeu, doivent être conformes au droit de l'UE;
- la section 2.5 fait explicitement mention de la nécessité de prévoir des garanties appropriées pour le transfert de données personnelles vers des pays tiers;
- des obligations de sécurité découlant des législations applicables en matière de protection des données sont explicitement mentionnées à la section 2.1;
- le respect de la vie privée dès la conception par les fabricants de produits et les fournisseurs de services TIC est considéré, à la section 2.4, comme une mesure qui sera encouragée.

19. Le CEPD constate toutefois que les sections relatives à la lutte contre la cybercriminalité et à la politique de cyberdéfense ne contiennent aucune mention spécifique des exigences en matière de respect de la vie privée et de protection des données. En tout état de cause, ainsi que la section 2.1.2 ci-dessous l'expliquera davantage, les obligations de protection de la vie privée et des données doivent également être prises en considération dans ces domaines d'action.

20. Le CEPD se félicite que le rôle et la participation des autorités chargées de la protection des données dans la lutte pour la cybersécurité soient mis en évidence, à la section 2.1, en ce qui concerne les actions de sensibilisation et la directive proposée sur la sécurité des réseaux et de l'information, et à la section 3.2 pour ce qui est des incidents ayant compromis des données à caractère personnel. Le CEPD souligne néanmoins que les autorités chargées de la protection des données ont un rôle à jouer dans toutes les actions de la stratégie de cybersécurité, et pas seulement dans celles où ce rôle a été explicitement mentionné. Cette question sera approfondie à la section 2.1.3 ci-dessous.

2.2. Commentaires spécifiques sur la stratégie de cybersécurité de l'UE

2.2.1. Délimiter le champ d'application des actions envisagées dans la stratégie de cybersécurité

21. La stratégie de cybersécurité vise à mettre en place une approche globale de la «cybersécurité» en abordant différents aspects de ses nombreux domaines tels que la cyber-résilience, la cybercriminalité et la cyberdéfense. Le CEPD admet que de nombreux aspects politiques, notamment les aspects techniques et autres, doivent être soigneusement examinés afin de garantir une protection adéquate des réseaux et systèmes informatiques, ainsi que des informations transmises dans ce cadre. Du point de vue de la protection des données, le CEPD estime qu'en contribuant à renforcer la sécurité dans l'espace numérique, les actions prévues dans le but de renforcer la cyber-résilience et la

lutte contre la cybercriminalité peuvent particulièrement aider à protéger les données à caractère personnel dans le cyberespace.

22. S'agissant de la taxonomie, et en particulier la définition de «cybersécurité», de «cyber-résilience», de «cybercriminalité» et de «cyberdéfense», le CEPD constate que la Commission s'est efforcée de définir certains de ces concepts aux fins de la communication conjointe (en particulier à ses notes de bas de page 4 et 5). Néanmoins, comme les notes de bas de page à la section 1.2 ci-dessus permettent de le déduire, les notions de «cyber-résilience», de «cybercriminalité» et de «cyberdéfense» ne sont pas nécessairement évidentes, ni précisément définies. Par conséquent, leur signification n'est pas toujours claire et, partant, le champ d'application des actions envisagées dans la communication conjointe ne l'est pas non plus. Bien que la communication soit un document politique non contraignant, il aurait été utile de définir ces notions plus précisément afin de parvenir à une compréhension commune claire de ce dont il est question et à une compréhension commune claire du champ d'application des actions envisagées dans la communication conjointe.

23. Du point de vue de la protection des données, la question de la terminologie revêt une importance toute particulière dès lors que ces termes sont utilisés comme justifications pour certaines mesures spéciales susceptibles de porter atteinte aux droits fondamentaux, notamment aux droits à la protection de la vie privée et des données. C'est particulièrement le cas des actions dans le domaine de la «cyber-résilience» et de la «cybercriminalité».

24. En ce qui concerne les actions destinées à améliorer la «cyber-résilience», le CEPD se félicite que la communication conjointe fasse référence à la législation en vigueur et proposée de l'Union dans le domaine de la sécurité des réseaux et de l'information. La directive proposée sur la sécurité des réseaux et de l'information visant à définir une approche intégrée de l'Union en matière de sécurité constitue une des principales actions de la communication conjointe dans ce domaine. Le CEPD fait remarquer que les actions envisagées dans ce domaine seraient prises dans le cadre juridique de l'UE (actuel ou futur) et que leur champ d'application serait dès lors clairement délimité par la législation[20].

25. Quant aux actions destinées à réduire la «cybercriminalité», la communication conjointe tente de fournir une définition du terme «cybercriminalité» dans une note au bas de la page 3. Le CEPD soutient cette tentative de définir ladite notion pour des raisons évidentes de sécurité juridique. Néanmoins, de l'avis du CEPD, la définition adoptée aux fins de la stratégie demeure assez vague et large, puisqu'elle englobe de manière générale tout type d'«*activités criminelles dont les ordinateurs et systèmes informatiques constituent soit l'arme soit la cible principale. […]*». La communication conjointe renvoie également, de façon non exhaustive, à plusieurs instruments juridiques de

[20] Il convient de noter que la législation proposée dans ce domaine, notamment la proposition de directive sur la sécurité des réseaux et de l'information présentée en lien avec la stratégie, est susceptible d'avoir une incidence sur la protection des données et doit dès lors être élaborée avec précaution, de manière à éviter toute atteinte illégale aux droits au respect de la protection de la vie privée et à la protection des données.

l'Union dans ce domaine[21]. Il convient toutefois de souligner que la législation de l'Union n'aborde que certains aspects très spécifiques des crimes commis en ligne[22] et qu'il n'existe pas encore de cadre juridique unique proposant une définition globale des infractions couvertes par le terme «cybercriminalité». En l'absence de définition commune de la notion de «cybercriminalité» dans le cadre juridique de l'Union, plusieurs mesures envisagées dans la stratégie et relatives à la lutte contre la «cybercriminalité» (comme les mesures destinées à renforcer la coopération entre les organes judiciaires) ne sont pas clairement liées à des infractions précises et bien définies.

26. La communication conjointe cite aussi les dispositions de la convention du Conseil de l'Europe sur la cybercriminalité de 2001, également appelée convention de Budapest, qui fournit un cadre approprié à l'adoption d'une législation nationale pour combattre la cybercriminalité. La convention de Budapest énumère toute une série d'infractions qui seraient englobées dans la notion de «cybercriminalité», telles que les infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques; les infractions informatiques; les infractions se rapportant au contenu; et les infractions liées aux atteintes au droit d'auteur et aux droits voisins. Cependant, outre le fait que cette liste reste assez vaste, comme indiqué dans la communication conjointe, la convention de Budapest n'a pas encore été ratifiée par tous les États membres et, par conséquent, les infractions couvertes par le terme «cybercriminalité» ne sont pas harmonisées dans le droit pénal des différents États membres de l'UE. Étant donné, par ailleurs, que les mesures prises dans le domaine de la répression sont davantage susceptibles de porter atteinte aux droits des personnes, il serait préférable de disposer d'une définition claire et *restrictive* de la «cybercriminalité», plutôt que d'une définition trop étendue.

2.2.2. Applicabilité de la législation sur la protection des données à tous les domaines d'action de la stratégie de cybersécurité de l'Union

27. Lorsque des politiques et législations de l'UE touchent au fonctionnement et à l'utilisation des réseaux et systèmes informatiques, par lesquels un nombre sans cesse croissant de données à caractère personnel sont traitées, il convient de reconnaître que les exigences légales en matière de protection de la vie privée et des données jouent un rôle essentiel et doivent nécessairement être prises en considération.

28. Comme indiqué au point 18 ci-dessus, le CEPD se félicite qu'il soit fait référence aux exigences légales en matière de respect de la vie privée et de protection des données en plusieurs points de la stratégie en tant que principes directeurs de la politique de cybersécurité, ainsi que dans les actions spécifiques, telles que celles relatives à la cyber-résilience, au développement des ressources industrielles et technologiques en matière de cybersécurité et à

[21] Voir en particulier la section 2.2., «Une législation solide et efficace», p. 9.

[22] Par exemple, la décision-cadre 2005/222/JAI du Conseil relative aux attaques visant les systèmes d'information[22]; la directive 2011/92/UE relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie; la décision-cadre 2001/413/JAI du Conseil concernant la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces.

l'instauration d'une politique internationale de l'Union européenne cohérente en matière de cyberespace.

29. Cependant, le CEPD constate avec regret l'absence de référence spécifique à la législation en matière de protection des données dans les sections portant sur la lutte contre la cybercriminalité (section 2.2)[23] et sur le développement d'une politique de cyberdéfense (section 2.3). Bien que la stratégie ne l'indique pas clairement, le CEPD note que bon nombre des actions prévues dans ces domaines sont susceptibles de comporter un traitement et un échange de données à caractère personnel.

30. Concernant la lutte contre la cybercriminalité, le CEPD souligne que les mesures qui sont envisagées dans la stratégie exigeront souvent la collecte, l'échange et l'analyse des données à caractère personnel des personnes (des noms et adresses IP, par exemple), y compris celles des victimes de cette criminalité et de suspects, dont le traitement entraîne des risques spécifiques pour le respect de la vie privée et la protection des données de ces personnes. Il est probable que ce soit le cas, par exemple, des mesures destinées à renforcer les moyens opérationnels et la coordination entre les organes chargés de l'application de la loi. En raison de sa nature intrusive et de l'incidence majeure qu'il peut avoir sur la vie de la personne, le traitement de données à caractère personnel dans le cadre de coopérations policières et judiciaires en matière pénale exige un niveau élevé de protection des données.

31. Dans le contexte d'enquêtes ou de poursuites concernant des infractions pénales, les échanges de données à caractère personnel entre services répressifs au sein de l'Union doivent actuellement respecter les exigences en matière de protection des données définies dans la décision 2008/977/JAI du Conseil[24]. Une proposition de directive régissant le traitement de données à caractère personnel dans le domaine de la coopération policière et judiciaire en matière pénale est en cours d'examen au Parlement européen et au Conseil[25] et devrait remplacer la décision-cadre du Conseil. Cet instrument deviendra la norme en matière de protection des données applicable au traitement de données par les services répressifs au sein de l'Union, régissant tant le traitement de données à caractère personnel par ces autorités que leur échange de données à caractère personnel avec d'autres destinataires.

[23] À l'exception du cas spécifique de l'ICANN, dans lequel les mesures destinées à étendre la responsabilité des bureaux d'enregistrement des noms de domaines et à garantir l'exactitude des informations sur les propriétaires de site web doivent se conformer au droit de l'Union, y compris aux règles sur la protection des données, voir la page 11.

[24] Décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, JO L 350 du 30.12.2008, p. 0060-0071.

[25] Proposition de directive du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, COM (2010) 010 final.

32. Ainsi que de précédents avis l'ont souligné[26], le CEPD est convaincu que les actions de lutte contre la cybercriminalité doivent être mises en place avec des garanties de protection des données soigneusement conçues, de façon à garantir que la surveillance et le traitement des données à caractère personnel par les services répressifs ne seront exercés que de manière strictement ciblée et proportionnée, ainsi qu'après un examen adéquat des droits de la personne concernée. Par exemple, les mesures destinées à renforcer les moyens opérationnels des services répressifs, y compris le Centre européen de lutte contre la cybercriminalité, doivent être mises en place conformément à une base juridique claire définissant avec suffisamment de précision la portée des moyens opérationnels à déployer (comme les types de crimes ciblés, les types d'outils opérationnels, le fait qu'ils impliquent ou non le traitement de données à caractère personnel et les modalités de ce traitement)[27]. Toute mesure de ce type ne devrait être prise qu'après avoir satisfait aux conditions de nécessité et de proportionnalité.

33. Quant au domaine de la politique de défense, le CEPD fait observer que dans une certaine mesure, plusieurs actions supposeront probablement un traitement de données à caractère personnel. Cela sera vraisemblablement le cas, par exemple, des mesures comme l'amélioration du partage d'information, l'échange d'information, les alertes rapides ou les interventions en cas d'incidents entre les acteurs civils et militaires au sein de l'Union, qui peuvent justifier l'échange de données à caractère personnel (comme les adresses IP et les noms des personnes de contact au sein des organisations concernées). Le traitement de données à caractère personnel dans ce domaine relève du champ d'application de la directive 95/46/CE. Des exemptions spécifiques visant à limiter le champ d'application des obligations et droits dans ce cas peuvent au besoin s'appliquer en vertu de l'article 13 de ladite directive.

34. Enfin, et de manière plus générale, le CEPD souligne l'importance de définir des garanties adéquates de protection des données lors de l'application des mesures destinées à améliorer la coordination entre les différentes parties prenantes. Le renforcement de la coordination entre les parties prenantes est envisagé dans de nombreux domaines de la stratégie, comme la cybercriminalité, la cyberdéfense et les relations extérieures de l'UE. Il convient de préciser en particulier si cette coordination peut exiger l'échange de données à caractère personnel concernant des personnes et, le cas échant, selon quelles modalités (par exemple entre les autorités compétentes seulement ou avec le secteur privé; au sein ou en dehors de l'Union). Il y a lieu de garantir que tout traitement de données à caractère personnel réalisé dans le contexte de mécanismes de coordination respecte les droits des personnes à la protection de la vie privée et des données. Dans une certaine mesure, la stratégie tient compte de la nécessité de respecter un niveau élevé de protection des données pour les transferts de données à caractère personnel vers des pays tiers (section 2.5), ce dont le CEPD se réjouit. Il convient

[26] Voir en particulier l'avis du CEPD relatif à la communication de la Commission européenne au Conseil et au Parlement européen concernant l'établissement d'un Centre européen de lutte contre la cybercriminalité, 29 juin 2012, disponible à la section Consultation du site web du CEPD, à l'adresse: www.edps.europa.eu.

[27] Voir aussi l'avis du CEPD sur le Centre européen de lutte contre la cybercriminalité, *ibid*.

toutefois de redoubler d'efforts lors de la mise en place des mécanismes de coordination envisagés dans la stratégie, de façon à ce que des garanties adéquates de protection des données soient définies en ce qui concerne les modalités d'échange de données à caractère personnel.

2.2.3. Rôle des autorités chargées de la protection des données dans la protection de la cybersécurité

35. Les autorités chargées de la protection des données (APD) jouent un rôle majeur dans le contexte de la cybersécurité. En tant que gardiennes des droits des personnes en matière de respect de la vie privée et de protection des données, les APD sont activement engagées dans la protection de leurs données à caractère personnel, que ce soit hors ligne ou en ligne. Dans le cadre de leur mandat, elles mènent des enquêtes, traitent des plaintes, réalisent des examens préalables et émettent des avis sur les opérations de traitement des données, y compris celles qui se déroulent en ligne ou passant par des réseaux de communication électronique[28]. À cet égard, il convient de souligner que la sécurité des données à caractère personnel constitue une part importante de leurs missions (par exemple en veillant au respect de l'article 17 de la directive 95/46/CE). Elles joueront également un rôle en suivant le traitement de données à caractère personnel effectué par les acteurs participant à la mise en œuvre de la stratégie de cybersécurité.

36. Le CEPD regrette dès lors que les APD ne soient pas mentionnées parmi les acteurs pertinents dans le domaine de la cybersécurité à la section 3 de la stratégie et dans le schéma présentant les principaux acteurs en page 19. Entre autres, la section 3 énumère les autorités compétentes en matière de SRI, les CERT, les services de maintien de l'ordre, les autorités de défense et l'ENISA en tant qu'entités assumant des responsabilités et un rôle particuliers, aux niveaux national, européen ou international. Cependant, comme souligné plus haut, les APD ont aussi un rôle à jouer dans le renforcement de la cybersécurité. Il faut pour ce faire que les acteurs susmentionnés associent les APD de manière adéquate mais aussi que de par leur mandat, les APD puissent agir en indépendance.

37. Cela signifie, d'une part, qu'en leur qualité d'organes de surveillance, les APD doivent être suffisamment associées à la mise en œuvre des mesures comportant un traitement de données à caractère personnel. Par exemple, les mesures à mettre en œuvre conformément à la section 2.1 «Parvenir à la cyber-résilience» comprennent le lancement d'un projet pilote financé par l'Union et consacré à la lutte contre les réseaux zombies et les logiciels malveillants. Dès lors que les mesures prises dans ce contexte peuvent porter atteinte au respect de la vie privée et à la protection des données à caractère personnel des personnes, le CEPD préconise que la mise en œuvre de ce projet pilote soit placée sous la surveillance des autorités compétentes en matière de protection des données.

[28] Leurs missions et pouvoirs sont définis à l'article 28 de la directive 95/46/CE.

38. D'autre part, les APD doivent être reconnues comme des acteurs importants dans le domaine de la cybersécurité, de façon à ce que la coopération envisagée entre les différents acteurs mentionnés à la section 3 de la stratégie s'étende aussi à elles. La stratégie reconnaît dans une certaine mesure la nécessité d'une coopération avec les APD lorsqu'un incident de sécurité semble avoir compromis des données à caractère personnel[29]. Néanmoins, cette coopération ne devrait pas être limitée au mandat des APD dans le domaine des enquêtes et de la surveillance des infractions concernant des données à caractère personnel. Les autorités compétentes en matière de SRI, les CERT, l'ENISA et les services répressifs doivent coopérer de façon générale avec les APD dans le cadre de l'échange de bonnes pratiques, ainsi que des actions de sensibilisation menées dans le domaine de la cybersécurité. De même, il convient d'associer le CEPD et les APD nationales de manière adéquate à la conférence de haut niveau qui se tiendra en 2014 pour examiner les progrès accomplis dans la mise en œuvre de la stratégie, dès lors qu'ils constituent des acteurs importants dans ce domaine.

3. ANALYSE DE LA DIRECTIVE PROPOSÉE

3.1. Commentaires généraux sur la directive proposée

3.1.1. Garantir que la mise en œuvre de la SRI respecte pleinement la législation en matière de protection des données

39. Le CEPD salue la référence explicite, contenue à l'article 1er, paragraphe 5, de la proposition, au cadre de l'UE applicable à la protection des données, en particulier la directive 95/46/CE et la directive 2002/58/CE[30]. Il se félicite également que le considérant 41 de la proposition dispose que la mise en œuvre de la directive proposée doive respecter la Charte des droits fondamentaux de l'Union européenne, et notamment le droit au respect de la vie privée et des communications et le droit à la protection des données à caractère personnel. Il constate que, bien que le considérant 39 mentionne la conformité au règlement (CE) n° 45/2001 relatif au traitement des données à caractère personnel par les institutions et organes de l'Union, cette référence est omise à l'article 1er, paragraphe 5. Le CEPD conseille aux législateurs d'inclure également une référence au règlement (CE) n° 45/2001 à l'article 1er, paragraphe 5, de la proposition.

40. Le CEPD accueille aussi favorablement le fait que la proposition tienne compte, dans une certaine mesure[31], de la proposition de règlement sur la protection des données[32], qui remplacera la directive 95/46/CE en définissant des règles générales applicables aux opérations de traitement des données par le secteur privé et les administrations publiques. L'article 1er, paragraphe 5, de la proposition souligne que le respect de ces règles devra être garanti lorsque

[29] Voir le point 19.
[30] Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques).
[31] Voir l'article 1er, paragraphe 5, et l'article 17 de la directive proposée.
[32] COM (2012) 11 final.

le règlement proposé sur la protection des données entrera en vigueur. L'article 17 exige des États membres qu'ils veillent, lorsqu'un incident de sécurité concerne des données à caractère personnel, à ce que les sanctions prévues soient conformes à celles définies dans le règlement relatif à la protection des données en vigueur à ce moment.

41. Il est toutefois regrettable que l'interaction des cadres juridiques actuel et futur sur la protection des données avec la directive proposée sur la sécurité des réseaux et de l'information n'ait pas été analysée plus en détail et que la proposition n'indique pas plus clairement comment cette interaction opérera. Ainsi que les sections ci-après l'analyseront plus en profondeur, la proposition laisse de nombreuses questions sans réponse sur des points tels que:

- la relation entre les obligations de sécurité contenues dans la directive et les autres obligations de sécurité prévues dans d'autres instruments juridiques (par exemple les actuel et futur cadres sur la protection des données, le cadre sur les télécommunications et le règlement proposé sur l'identification électronique et les services de confiance pour les transactions électroniques) et le niveau de sécurité que les opérateurs concernés doivent appliquer;
- les obligations des autorités compétentes en matière de SRI quant au niveau de confidentialité et de sécurité qu'elles doivent garantir concernant les données qu'elles reçoivent dans le cadre d'une procédure de notification d'un incident;
- le contenu des notifications d'incident et le fait qu'elles puissent ou non inclure des données à caractère personnel et, le cas échéant, lesquelles (à décider au moyen d'actes délégués);
- les modalités de l'interaction des autorités compétentes en matière de SRI avec les APD, ainsi qu'avec l'ENISA, lorsque l'incident met en jeu des données à caractère personnel.

42. En outre, le CEPD insiste sur la nécessité, qui découle de l'actuel cadre sur la protection des données ainsi que de la proposition de règlement sur la protection des données, d'intégrer le respect de la vie privée et la protection des données dès la conception et par défaut[33] lors de la conception et du fonctionnement des mécanismes prévus par la directive proposée[34]. Le CEPD préconise dès lors d'insérer dans la proposition une disposition visant à ce que la protection des données soit prise en considération à un stade précoce de la conception des mécanismes établis dans la proposition et tout au long du cycle de vie des processus, procédures, organisations, techniques et infrastructures concernés. Il convient d'ajouter un considérant pour expliquer cette nécessité également dans le contexte de la proposition de règlement sur la protection des données.

3.1.2. Champ d'application de la proposition

[33] Voir l'article 23 de la proposition de règlement général sur la protection des données.
[34] Voir aussi l'avis du CEPD sur la communication de la Commission relative à «Une stratégie numérique pour l'Europe: faire du numérique un moteur de la croissance européenne», 10 avril 2013, disponible à la section Consultation du site web du CEPD à l'adresse: www.edps.europa.eu.

43. La directive proposée exige, entre autres choses, que les États membres imposent des obligations de sécurité aux administrations publiques et aux «acteurs du marché» définis à l'article 3, paragraphe 8. La définition d'«acteurs du marché» couvre les principaux prestataires de services de la société de l'information et les opérateurs d'infrastructure critique dans le domaine de l'énergie, des transports, des services bancaires, des bourses de valeurs, des services internet et de la santé. Une liste non exhaustive des acteurs du marché couverts par le champ d'application de la proposition figure à l'annexe II, qui reprend spécifiquement les principaux prestataires de services de la société de l'information suivants: les plateformes de commerce électronique, les passerelles de paiement par internet, les réseaux sociaux, les moteurs de recherche, les services d'informatique dématérialisée et les magasins d'applications en ligne.

44. Bien que l'obligation, imposée dans la proposition, de garantir que le secteur privé et les administrations publiques respectent des exigences minimales en matière de sécurité soit accueillie positivement, le CEPD fait observer que plusieurs obligations de sécurité sont déjà définies dans le cadre juridique de l'Union applicable aux fournisseurs de réseaux et de services de communications électroniques en vertu de la directive-cadre 2002/21/CE et aux responsables du traitement des données en vertu de la législation sur la protection des données[35]. Le CEPD estime qu'une approche intégrée de la sécurité s'impose afin d'atténuer les risques en matière de SRI, ce qui, à son tour, contribue aussi à atténuer les risques pour le respect de la vie privée et la protection des données. Cette approche est d'autant plus importante dans des environnements numériques de plus en plus interconnectés, où des interférences accidentelles ou intentionnelles peuvent facilement se propager d'un système à l'autre. Comme indiqué au point 13 ci-dessus, le CEPD est d'avis que l'obligation de sécurité prévue dans la législation sur la protection des données est probablement l'obligation de sécurité des réseaux et de l'information la plus complète au titre du droit de l'Union. À cet égard, la directive proposée n'offre pas encore une approche pleinement intégrée de la sécurité, ainsi qu'il sera démontré ci-après.

45. Premièrement, la proposition ne définit pas clairement ni de façon exhaustive quels acteurs du marché seraient couverts par le champ d'application de la proposition. Elle définit une liste non exhaustive d'acteurs du marché concernés, laquelle peut être étendue à d'autres acteurs, de façon non harmonisée, par les États membres. L'on peut également se demander pourquoi certains secteurs qui jouent un rôle majeur dans la sécurité des réseaux et de l'information ne figurent pas sur cette liste, comme les fabricants de matériel informatique et de logiciels ou les fournisseurs de logiciels et de services de sécurité. En outre, le libellé actuel de la proposition n'indique pas tout à fait clairement si les institutions et organes de l'UE relèveront ou non du champ d'application de la proposition. Le considérant 39 semble sous-entendre que c'est le cas, toutefois l'article 1er de la proposition devrait l'indiquer plus clairement. Le CEPD conseille par conséquent aux législateurs

[35] Voir la note de bas de page n° 13.

d'introduire plus de clarté et de sécurité à l'article 3, paragraphe 8, sur la définition des acteurs du marché couverts par le champ d'application de la proposition et de dresser une liste exhaustive reprenant tous les acteurs concernés, afin de garantir une approche pleinement harmonisée et intégrée de la sécurité au sein de l'Union. Le CEPD préconise en outre de préciser à l'article 1er, paragraphe 2, point c), que la proposition s'applique aussi aux institutions et organes de l'UE.

46. Deuxièmement, l'adoption d'une approche intégrée de la sécurité est aussi entravée par le fait que plusieurs acteurs sont expressément exclus du champ d'application de la proposition. L'article 1er, paragraphe 3[36], de la proposition tient compte des obligations légales actuelles déjà imposées aux réseaux de communication publics et aux services de communications électroniques accessibles au public au sens de la directive 2002/21/CE. L'article 1er, paragraphe 3, les exclut dès lors du champ d'application de la proposition. L'article 1er, paragraphe 3, exclut également les fournisseurs de services de confiance, dès lors qu'ils seront soumis aux obligations définies dans la proposition de règlement sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur[37]. Ces exclusions peuvent sembler porter à confusion, dans la mesure où elles laissent plusieurs cadres juridiques coexister, sans préciser comment ils interagissent l'un avec l'autre. En particulier, il convient de préciser si le niveau de sécurité requis par la directive 2002/21/CE devrait aussi être applicable aux acteurs couverts par le champ d'application de la directive proposée. Le CEPD recommande qu'un rôle plus horizontal pour cette proposition soit reconnu en ce qui concerne les exigences en matière de sécurité, en prévoyant explicitement à l'article 1er qu'elle doit s'appliquer sans préjudice des règles plus détaillées, existantes ou futures, dans des domaines spécifiques (comme celles qui seront définies concernant les fournisseurs de services de confiance dans la proposition de règlement sur l'identification électronique).

3.2. Commentaires spécifiques sur la directive proposée

3.2.1. Sur les définitions fournies dans la directive proposée

47. Il convient de préciser si la définition de «réseau et système informatique» donnée à l'article 3, paragraphe 1, vise à couvrir les réseaux locaux privés qui ne sont pas connectés à l'internet. Dès lors que la Commission ne fournit aucune justification pour imposer des obligations couvrant les réseaux privés isolés, cela semblerait indiquer que les réseaux privés ne relèvent pas du champ d'application de la proposition. Il faudrait le préciser à l'article 3, paragraphe 1.

48. La définition d'«incident» donnée à l'article 3, paragraphe 4, doit être davantage précisée, également en lien avec la définition de «sécurité» contenue à l'article 3, paragraphe 2, et avec la définition de «risque» à

[36] Voir aussi le considérant 5.
[37] Voir *ibid*.

l'article 3, paragraphe 3. Par exemple, ces définitions ne permettent pas de savoir si l'attaque d'un système informatique peut être considérée comme un incident si l'auteur de cette attaque ne parvient pas à compromettre sa sécurité. À cet égard, il y a lieu de tenir compte de la définition de «violation de données à caractère personnel» contenue à l'article 2, point i), de la directive «vie privée et communications électroniques»[38] et à l'article 4, paragraphe 9, de la proposition de règlement sur la protection des données, où la violation doit entraîner une conséquence (par exemple l'altération, la perte, etc.).

3.2.2. Sur les obligations des États membres en ce qui concerne la prévention et la gestion de risques et incidents ainsi que les interventions en cas d'évènement de ce type

49. L'article 5, paragraphes 1 et 2, exige des États membres qu'ils adoptent une stratégie nationale en matière de SRI et un plan national de coopération en matière de SRI. L'article 5, paragraphe 2, précise les exigences relatives aux plans nationaux de coopération en matière de SRI. En particulier, il prévoit l'élaboration d'un plan d'évaluation des risques permettant de recenser les risques et d'évaluer l'impact d'incidents potentiels. Le CEPD estime que l'obligation d'élaborer un «plan d'évaluation des risques» est trop étriquée, dès lors que ce libellé n'inclut pas les autres activités nécessaires dans le cadre de la gestion des risques relatifs à la sécurité de l'information[39], comme par exemple, pour ne citer que les plus importantes, la hiérarchisation et le traitement des risques (transfert, évitement, atténuation, etc.), y compris les critères pour le choix de contre-mesures possibles et l'acceptation des risques résiduels. En lieu et place, afin d'utiliser un libellé incluant toutes les actions nécessaires, le CEPD recommande que cette exigence consiste à «établir et maintenir un cadre de gestion des risques» (ce qui, bien entendu, impliquerait également une phase d'évaluation des risques).

50. L'article 6, paragraphe 1, de la proposition prévoit la désignation d'une autorité nationale compétente en matière de sécurité des réseaux et systèmes informatiques (ci-après l'«autorité compétente en matière de SRI»). Le CEPD salue l'obligation explicite imposée par l'article 6, paragraphe 5, et par l'article 15, paragraphe 5, à l'autorité compétente en matière de SRI de consulter l'autorité chargée de la protection des données et, le cas échéant, de coopérer avec elle. Le CEPD est d'avis que cette coopération est fondamentale pour garantir, d'une part, un niveau élevé de sécurité et, d'autre part, la prise en considération du respect de la vie privée et de la protection des données dans le cadre des actions déployées dans le but de protéger la sécurité des réseaux et systèmes informatiques. Le CEPD appelle par ailleurs à la participation, dans la pratique et dès qu'elle est nécessaire, des autorités

[38] L'article 2, point i), de la directive 2002/58/CE, telle que modifiée par la directive 2009/136/CE, dispose qu'une violation de données à caractère personnel «est une violation de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisés de données à caractère personnel transmises, stockées ou traitées d'une autre manière en relation avec la fourniture de services de communications électroniques accessibles au public dans la Communauté».

[39] Voir par exemple la norme ISO/IEC 27005:2008 sur la gestion des risques en sécurité de l'information.

chargées de la protection des données dans la définition et la mise en œuvre des stratégies nationales et des plans de coopération en matière de SRI.

51. L'article 7 impose la mise en place, par chaque État membre, d'une équipe d'intervention en cas d'urgence informatique (CERT), laquelle peut être établie au sein de l'autorité compétente. Le CEPD préconise d'indiquer clairement à l'annexe I que les exigences en matière de protection des données font aussi partie des exigences essentielles auxquelles les CERT doivent se conformer. Le CEPD constate en outre avec satisfaction que, par l'intermédiaire des autorités nationales compétentes qui les supervisent, les CERT peuvent au besoin réclamer la coopération spécifique des autorités chargées de la protection des données dans l'accomplissement de leurs missions, conformément à l'article 6, paragraphe 5, de la proposition.

3.2.3. Sur les exigences de sécurité proposées pour les acteurs du marché et les administrations publiques

52. Le CEPD se félicite que des exigences de sécurité et de notification soient imposées aux acteurs du marché et aux administrations publiques à l'article 14, qui vise à promouvoir une culture de gestion des risques et à faire en sorte que les incidents les plus graves soient signalés.
53. L'article 14, paragraphe 2, exige des administrations publiques et des acteurs du marché qu'ils notifient à l'autorité compétente en matière de SRI les incidents qui ont un impact significatif sur la sécurité des services essentiels qu'ils fournissent. Néanmoins, les circonstances dans lesquelles une notification est requise, ainsi que le contenu et le format de la notification, ne sont pas définis dans la proposition elle-même, mais le seront au moyen d'actes délégués et d'actes d'exécution. Le CEPD souligne qu'en n'introduisant pas des dispositions substantielles sur ces aspects, le texte de la proposition n'apporte pas la sécurité juridique suffisante aux acteurs du marché et aux administrations publiques couverts par le champ d'application de cette notification. Il convient en outre de préciser dans la proposition les types de données qui peuvent être collectées (comme le nom des membres du personnel en charge de la sécurité) et si la notification et ses documents explicatifs incluront ou non des détails sur les données à caractère personnel affectées par un incident de sécurité spécifique et, le cas échéant, dans quelle mesure. Le CEPD rappelle que les données à caractère personnel ne peuvent être transmises qu'en cas de stricte nécessité pour la gestion de l'incident. Le CEPD recommande que ces aspects de la notification soient définis plus en détail dans le texte de la proposition elle-même (voir l'analyse plus détaillée contenue à la section 3.2.4.) et que des garanties appropriées soient établies afin d'assurer une protection adéquate des données traitées par les autorités compétentes en matière de SRI (qu'il s'agisse de données à caractère personnel, de données sensibles ou de données confidentielles).

54. Le CEPD se félicite que l'article 15, paragraphe 5, prévoie explicitement une coopération étroite des autorités compétentes en matière de SRI avec les autorités chargées de la protection des données en cas d'incident portant atteinte à des données à caractère personnel. Le CEPD conseille de préciser à l'article 14 que les notifications d'incident visées à l'article 14, paragraphe 2,

s'appliquent sans préjudice des obligations de notification des violations de données à caractère personnel imposées par la législation applicable en matière de protection des données (à savoir la directive «vie privée et communications électroniques» et la proposition de règlement général sur la protection des données). Une disposition similaire est présente à l'article 15, paragraphe 2, de la proposition de règlement sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur[40]. En outre, le CEPD préconise que les modalités essentielles de la notification aux autorités compétentes en matière de SRI d'incidents portant atteinte à des données à caractère personnel soient expressément définies dans une disposition de la proposition (voir les commentaires plus approfondis formulés à la section 3.2.4.). Il convient de veiller à ce que la procédure respecte la compétence des autorités chargées de la protection des données (ou des autres organes réglementaires nationaux visés dans la directive «vie privée et communications électroniques») dans ce cas.

55. La proposition prévoit en outre la divulgation au public d'informations relatives à l'incident. L'article 14, paragraphe 4, dispose que «*L'autorité compétente peut informer le public, ou demander aux administrations publiques et aux acteurs du marché de le faire, lorsqu'elle juge qu'il est dans l'intérêt général de divulguer les informations relatives à l'incident*». Le CEPD est d'avis que, par principe, ces informations ne devraient contenir aucune donnée à caractère personnel des personnes concernées par l'incident. Au sens de l'article 14, paragraphe 4, dans la plupart des cas, l'intérêt général ne devrait être effectivement poursuivi en ne divulguant que des informations anonymes ou effectivement rendues anonymes. Cependant, si ces informations devaient inclure des données à caractère personnel, le CEPD indique que la décision de divulguer des données à caractère personnel doit reposer sur un juste équilibre entre les différents intérêts en jeu. À cet égard, la Cour de justice a souligné dans l'affaire *Schecke*[41] que la publication de données à caractère personnel (comme les noms et les montants précis perçus par les bénéficiaires de fonds de l'UE) constituait une atteinte aux droits au respect de la vie privée et à la protection des données des personnes concernées et ne pouvait se faire que sur la base d'une analyse de la nécessité et de la proportionnalité par rapport à l'objectif poursuivi.

56. Enfin, le CEPD constate que l'article 14, paragraphe 8, exclut les micro-entreprises des exigences de sécurité et de notification d'incidents définies à l'article 14, paragraphes 1 et 2. Le CEPD fait observer que certains des acteurs du marché repris à l'annexe II de la directive proposée peuvent être des startups dont les activités en tant que fournisseurs de services de la société de l'information connaissent une croissance rapide (de nouveaux réseaux sociaux, par exemple) et qui jouent déjà un rôle majeur dans leur secteur de marché. L'actuelle définition de «micro-entreprise»[42] peut ne pas tenir compte de

[40] COM (2012) 238 final, op.cit.
[41] Affaires jointes C-92/09 et C-93/09, *Schecke*, points 56 à 64.
[42] Recommandation 2003/361/CE de la Commission du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises, qui définit une micro-entreprise «*comme une entreprise qui occupe moins de 10 personnes et dont le chiffre d'affaires annuel ou le total du bilan annuel n'excède pas 2 millions d'euros*».

certains d'entre eux. Le CEPD conseille aux législateurs de modifier l'article 14, paragraphe 8, afin que l'exclusion des micro-entreprises ne s'applique pas aux acteurs qui jouent un rôle crucial dans la fourniture de services de la société de l'information, compte tenu par exemple de la nature des informations qu'ils traitent (des données biométriques ou des données sensibles, par exemple).

3.2.4. *Sur le partage d'informations relatives aux incidents et menaces liés à la SRI avec les autorités compétentes en matière de SRI et au sein du réseau de coopération*

57. Conformément à l'obligation de notification visée à l'article 14, les acteurs du marché et les administrations publiques sont tenus de partager des informations sur les incidents de SRI avec l'autorité compétente en matière de SRI. Si le contenu de cette notification et les types de données à communiquer à l'autorité compétente en matière de SRI ne sont pas précisés dans la proposition, il est toutefois possible d'anticiper que la notification contiendra des informations qui sont considérées comme confidentielles, ainsi que des données à caractère personnel, y compris des données sensibles.

58. Les données à caractère personnel échangées avec les autorités compétentes en matière de SRI peuvent par exemple comprendre les noms et les coordonnées du personnel de sécurité des organisations notifiantes, ainsi que des adresses IP qui sont fournies dans le cadre des données techniques liées à l'incident. Ces adresses IP peuvent se rapporter à des personnes concernées par l'incident, ainsi qu'à des personnes pouvant à un moment donné être soupçonnées d'être responsables de l'incident. Même si l'organisation notifiante et l'autorité compétente en matière de SRI ne sont pas nécessairement en mesure de relier directement l'adresse IP à une personne identifiée, ces adresses IP n'en demeurent pas moins des données à caractère personnel dans la mesure où elles permettent l'identification *indirecte* des personnes qui se trouvent derrière ces adresses (par l'intermédiaire, notamment, du fournisseur de services internet). En outre, cette identification pourrait être réclamée à un moment ou l'autre de l'enquête, que ce soit par l'autorité compétente en matière de SRI ou par les autorités répressives auxquelles ces données peuvent être transmises par la suite conformément à l'article 10, paragraphe 4, et à l'article 15, paragraphe 4. Le CEPD souligne que le traitement de données à caractère personnel par les autorités compétentes en matière de SRI ne peut être considéré comme légal que s'il repose sur une base juridique appropriée au sens de l'article 7 de la directive 95/46/CE et qu'il n'est pas excessif au regard des objectifs à atteindre (principe de proportionnalité). Ce point sera approfondi ci-après.

59. Le CEPD constate également que toutes les informations collectées par les autorités compétentes en matière de SRI peuvent ensuite être partagées avec d'autres destinataires. L'article 15, paragraphe 4, dispose que les autorités compétentes en matière de SRI doivent notifier aux services répressifs les incidents pouvant constituer une infraction pénale grave. Les informations collectées par les autorités compétentes en matière de SRI peuvent également être partagées au sein d'un réseau de coopération, composé des autorités

compétentes en matière de SRI au sein de l'Union et de la Commission. L'objectif de ce réseau de coopération consiste à permettre un échange d'informations structuré et coordonné, ainsi qu'une détection coordonnée (via la procédure d'«alerte rapide» visée à l'article 10) et une intervention coordonnée (via la procédure d'intervention coordonnée visée à l'article 11) en matière de SRI. D'autres organismes de l'UE concernés, dont l'ENISA (article 8, paragraphe 2), le Centre européen de lutte contre la cybercriminalité au sein d'Europol et les autorités chargées de la protection des données [article 8, paragraphe 3, point f)] peuvent être amenés à porter assistance au réseau de coopération et des informations peuvent également être partagées avec eux. Les points ci-dessous analyseront plus en profondeur s'il existe une base juridique suffisante pour le partage de données à caractère personnel avec ces autres destinataires, et quelles sont les garanties à mettre en place pour protéger les droits de la personne dans le contexte de ces échanges.

Base juridique pour le traitement et le partage de données à caractère personnel en vertu de la directive proposée

60. L'article 1er, paragraphe 6, de la directive proposée reconnaît que les notifications d'incidents de SRI et le partage d'informations au sein du réseau de coopération peuvent nécessiter le traitement de données à caractère personnel. Conformément à ces dispositions, le traitement de données à caractère personnel à ces fins est justifié en vertu de l'article 7 de la directive 95/46/CE comme étant «*nécessaire à l'exécution de la mission d'intérêt public qui est celle de la présente directive*». Le considérant 39 de la directive proposée ajoute que ce traitement «*ne constitue pas, au regard de ces objectifs légitimes, une intervention disproportionnée et intolérable qui porterait atteinte à la substance même du droit à la protection des données à caractère personnel*». Par conséquent, l'article 1er, paragraphe 6, dispose que ce traitement «*est autorisé par l'État membre conformément à l'article 7 de la directive 95/46/CE et à la directive 2002/58/CE, tels que transposés en droit national*».

61. L'article 7 de la directive 95/46/CE cite six motifs juridiques spécifiques et exclusifs susceptibles de justifier le traitement de données à caractère personnel. Néanmoins, le considérant 39 et l'article 1er, paragraphe 6, de la proposition ne précisent pas lequel de ces motifs juridiques justifierait le traitement de données à caractère personnel par les autorités compétentes afin de gérer des incidents de SRI et de partager des informations avec d'autres autorités compétentes. De l'avis du CEPD, ce traitement peut être justifié au titre de l'article 7, point e), de la directive 95/46/CE dans la mesure où il est «*nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées*». Il recommande dès lors de préciser à l'article 1er, paragraphe 6, de la proposition que le traitement est justifié en vertu de l'article 7, point e), de la directive 95/46/CE, dans la mesure où il est nécessaire à l'exécution de la mission d'intérêt public qui est celle de la directive proposée.

62. Le CEPD insiste toutefois sur le fait qu'il convient de garantir le plein respect des principes de nécessité et de proportionnalité, afin que seules les données strictement nécessaires à l'objectif visé soient traitées. Le respect de ces principes s'applique non seulement aux administrations publiques et aux acteurs du marché qui subissent l'incident et traitent les données, mais aussi: i) au point de collecte des données à caractère personnel par les autorités compétentes en matière de SRI (c'est-à-dire dans le formulaire de notification de l'incident); ii) lors de la conception de l'échange structuré d'informations via le réseau de coopération; et iii) pour la transmission ultérieure de données à caractère personnel à d'autres destinataires (en particulier aux autorités compétentes nationales et de l'UE).

Garantir la proportionnalité du traitement et du partage de données à caractère personnel

63. Au point de collecte, le formulaire de notification devrait préciser quelles données à caractère personnel seront collectées de manière structurelle (par exemple, le nom de la personne responsable de la sécurité au sein de l'organisation). Il devrait également préciser si, et sous quelles conditions, les organisations doivent inclure les coordonnées des adresses IP obtenues dans les rapports techniques, en décrivant ce qui s'est produit au niveau des systèmes et réseaux informatiques au moment de l'incident. En outre, il doit indiquer si des données à caractère personnel ont été compromises.

64. Si la protection de données à caractère personnel a été mise en péril, des procédures spécifiques doivent être mises en place afin de guider la gestion de ces cas par les autorités compétentes en matière de SRI, de concert avec les autorités chargées de la protection des données. De l'avis du CEPD, il faut veiller à ce que l'ampleur du traitement des données à caractère personnel réalisé par les autorités compétentes en matière de SRI soit conforme à leur mandat et n'interfère pas avec les missions des autorités chargées de la protection des données. Tandis que de par leur mandat, les autorités chargées de la protection des données sont habilitées à accéder, si nécessaire[43], à des données à caractère personnel pour les aider à évaluer la violation de ces données et à y remédier, la mission des autorités compétentes en matière de SRI n'implique pas forcément la nécessité qu'elles connaissent dans le détail les données à caractère personnel mises en péril. Compte tenu du fait que le traitement de données à caractère personnel par les APD dans le cadre d'enquêtes pour violation de données ne s'effectue que s'il est nécessaire, les autorités compétentes en matière de SRI – dont le mandat n'est pas d'enquêter sur des violations de données à caractère personnel – ne devraient a fortiori être autorisées à collecter et à traiter ce type de données dans le cadre d'un incident de sécurité que si cette collecte et ce traitement s'avèrent strictement nécessaires.

65. Le CEPD recommande que tous les aspects susmentionnés soient précisés dans la proposition, à tout le moins dans les grandes lignes. Actuellement,

[43] Comme indiqué en particulier à l'article 8, paragraphe 3, de la directive 95/46/CE qui définit les pouvoirs des APD et à l'article 15 bis, paragraphe 3, de la directive 2002/58/CE «vie privée et communications électroniques», telle que modifiée par la directive 2009/136/CE.

l'article 14, paragraphe 7, prévoit que la Commission adopte des actes d'exécution définissant les formats et les procédures applicables aux fins de la notification. Cependant, des exigences spécifiques devraient être introduites à l'article 14 afin de: i) préciser les types de données à caractère personnel qui doivent être notifiées aux autorités compétentes en matière de SRI (comme indiqué aux points 53 et 63 ci-dessus); ii) fournir des garanties quant au traitement des données à caractère personnel par les autorités compétentes en matière de SRI, de façon à ce que celui-ci reste proportionné à l'objectif poursuivi; et iii) donner des détails sur les procédures relatives à la coopération des autorités compétentes en matière de SRI avec les APD dans les cas où l'incident porte sur des données à caractère personnel (comme la façon dont les APD sont informées, le type d'informations à leur fournir, la manière dont elles doivent coordonner leur intervention par rapport à l'incident et les sanctions éventuelles).

66. En ce qui concerne l'échange ultérieur de données à caractère personnel par les autorités compétentes en matière de SRI avec d'autres destinataires (au sein du réseau de coopération ou en dehors), il convient de garantir que: i) les données à caractère personnel ne seront divulguées qu'à des destinataires dont le traitement est nécessaire à l'accomplissement de leur mission conformément à une base juridique appropriée; et ii) ces informations sont limitées au strict nécessaire à l'accomplissement de leur mission. À cet égard, la divulgation, par l'autorité compétente en matière de SRI, d'une partie ou de la totalité des données à caractère personnel en sa possession n'est pas forcément indispensable à la coopération avec d'autres autorités compétentes, eu égard à leur mission et leur mandat. Une évaluation adéquate doit être effectuée au cas par cas par l'autorité compétente en matière de SRI avant de divulguer toute donnée à caractère personnel à un destinataire externe afin de déterminer si, et dans quelle mesure, des données à caractère personnel doivent être transmises à ce destinataire. Le CEPD recommande l'ajout, dans la proposition, de dispositions spécifiques mettant ces principes en évidence.

67. Une attention particulière doit en outre être accordée au respect du principe de la limitation de la finalité. Si l'entité qui fournit au départ les données au réseau de partage d'informations ne peut déterminer avec une certitude suffisante à quelles fins l'information sera traitée et fera l'objet de transferts ultérieurs, elle peut, dans un premier temps, être obligée de limiter très strictement la fourniture de données à caractère personnel aux informations liées à l'incident et ne fournir d'autres détails qu'en réponse à des demandes individuelles justifiées, ce qui est susceptible de réduire considérablement l'utilité du réseau.

Autres exigences relatives au traitement et à l'échange d'informations

68. Le CEPD souligne que d'autres exigences en matière de protection des données, telles que définies dans le droit applicable, doivent aussi être respectées. Bon nombre de ces exigences devraient être explicitement énoncées dans la proposition, afin de fournir des garanties effectives. Par exemple, les autorités compétentes en matière de SRI doivent veiller à ce que les données à caractère personnel ne soient pas conservées plus longtemps que

ce qui est nécessaire pour atteindre les objectifs pour lesquels elles ont été collectées. Pour ce faire, il faudra définir un délai approprié applicable à la conservation des données à caractère personnel, conformément aux objectifs définis dans la directive proposée, notamment en ce qui concerne la conservation des données par les autorités compétentes en matière de SRI et au sein de l'infrastructure sécurisée du réseau de coopération.

69. Par ailleurs, l'information de la personne concernée prévue aux articles 10 et 11 de la directive 95/46/CE quant à l'identité du responsable du traitement, aux finalités du traitement, aux types de données traitées, aux destinataires des données et à ses droits à la protection des données serait mieux respectée si des modalités claires sur ces aspects étaient définies dans le texte de la proposition elle-même. Ces dispositions détaillées devraient être ajoutées à la proposition, de même qu'un avertissement rappelant aux autorités compétentes en matière de SRI qu'elles restent responsables de rendre ces informations sur le traitement des données à caractère personnel facilement accessibles, par exemple en publiant leur politique en matière de respect de la vie privée sur leur site web.

70. Le CEPD considère en outre qu'il est de la plus haute importance qu'à tout moment du traitement, les données traitées par les autorités compétentes en matière de SRI, puis partagées avec d'autres destinataires, soient suffisamment sécurisées. Le CEPD se félicite que l'article 9 prévoie la mise en place d'un système sécurisé d'échange d'informations pour appuyer le réseau de coopération dans l'échange d'informations sensibles et confidentielles. Le CEPD regrette toutefois que la proposition ne contienne aucune disposition spécifique quant au niveau de sécurité que les autorités compétentes en matière de SRI doivent respecter quand elles traitent des données. Le CEPD conseille aux législateurs d'inclure à la proposition une disposition spécifique relative à la sécurité des informations collectées, traitées et échangées par les autorités compétentes en matière de SRI. Une référence aux exigences de sécurité visées à l'article 17 de la directive 95/46/CE doit être spécifiquement introduite en ce qui concerne la protection des données à caractère personnel traitées par les autorités compétentes en matière de SRI.

71. Conformément à l'article 9, paragraphe 2, des critères relatifs à la participation des États membres au système sécurisé d'échange d'informations peuvent être définis par la Commission au moyen d'actes délégués. Le CEPD souligne qu'il convient de définir des critères pour veiller à ce qu'un niveau élevé de sécurité et de résilience soit garanti par tous les participants aux systèmes d'échange d'informations, et ce à toutes les étapes du traitement. Le CEPD insiste sur le fait que la Commission devrait être tenue par ces critères pour participer en tant que responsable du traitement au système sécurisé d'échange d'informations (en particulier dans la mesure où, conformément à l'article 8, la Commission participera activement au réseau en recevant et en échangeant des informations). Parmi ces critères, les États membres et la Commission doivent prendre des mesures appropriées de confidentialité et de sécurité afin de protéger les données à caractère personnel traitées dans le cadre du système, conformément aux articles 16 et 17 de la directive 95/46/CE et aux articles 21

et 22 du règlement (CE) n° 45/2001. Le CEPD recommande que cette exigence soit soulignée à l'article 9 de la proposition.

72. Le CEPD constate que la directive proposée ne définit pas explicitement les modalités relatives à la création, à l'exploitation et à la gestion du système d'échange d'informations. Il convient, notamment, de préciser si la Commission jouera un rôle dans l'établissement, dans le fonctionnement et dans la maintenance de l'infrastructure sécurisée. Ce rôle aura également une incidence sur les responsabilités de la Commission en ce qui concerne le traitement des données à caractère personnel effectué par l'intermédiaire de cette infrastructure, conformément au règlement (CE) n° 45/2001. En conséquence, le CEPD recommande d'ajouter à l'article 9 une description des rôles et responsabilités respectifs de la Commission et des États membres dans la création, l'exploitation et la maintenance du système sécurisé d'échange d'informations. Le CEPD recommande que la proposition définisse des exigences minimales de sécurité et des principes de protection des données pour la qualité des données en ce qui concerne l'exploitation du système d'échange d'informations. Le CEPD suggère en outre que la proposition prévoie explicitement que la conception du système soit conforme aux principes de protection des données dès la conception et par défaut et de sécurité dès la conception[44].

73. Enfin, le CEPD se réjouit du fait que l'article 13 prévoie que toute coopération des membres du réseau de coopération avec des partenaires internationaux doit s'effectuer sur la base d'accords internationaux, lesquels doivent assurer un niveau suffisant de protection des données à caractère personnel diffusées au sein du réseau de coopération. Le CEPD rappelle que tout transfert de données à caractère personnel vers des destinataires situés en dehors de l'Union doit être conforme aux articles 25 et 26 de la directive 95/46/CE, et à l'article 9 du règlement (CE) n° 45/2001.

4. CONCLUSIONS

74. Le CEPD se félicite que la Commission et la haute représentante de l'Union européenne pour les affaires étrangères et la politique de sécurité aient présenté une stratégie globale de cybersécurité assortie d'une proposition de directive concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et de l'information (SRI) dans l'UE. Cette stratégie vient compléter les actions politiques déjà mises en œuvre par l'Union dans le domaine de la sécurité des réseaux et de l'information.

75. Le CEPD se réjouit du fait que la stratégie aille au-delà de l'approche traditionnelle consistant à opposer sécurité et respect de la vie privée en prévoyant une reconnaissance explicite du respect de la vie privée et de la protection des données en tant que valeurs essentielles qui devraient inspirer la politique de cybersécurité dans l'UE et au niveau international. Le CEPD note

[44] Voir le texte de la communication conjointe à la page 28 quant aux recommandations aux parties prenantes publiques et privées sur l'adhésion aux principes de sécurité et de respect de la vie privée dès la conception.

que la stratégie de cybersécurité et la directive proposée sur la sécurité des réseaux et de l'information peuvent jouer un rôle fondamental en contribuant à garantir la protection des droits des personnes au respect de la vie privée et à la protection des données dans l'environnement en ligne. En même temps, il convient de veiller à ce qu'elles ne soient pas à l'origine de mesures qui constitueraient des atteintes illégales aux droits des personnes au respect de la vie privée et à la protection des données.

76. Le CEPD salue également le fait que la protection des données soit mentionnée dans plusieurs parties de la stratégie et qu'elle soit prise en considération dans la directive proposée sur la sécurité des réseaux et de l'information. Il regrette toutefois que ni la stratégie, ni la directive proposée ne soulignent davantage la contribution apportée par la législation existante et à venir en matière de protection des données à la sécurité et ne garantissent pleinement que toutes les obligations découlant de la directive proposée ou d'autres éléments de la stratégie soient complémentaires avec les obligations de protection des données et qu'elles ne se chevauchent pas, ni ne se contredisent.

77. Par ailleurs, le CEPD constate que, du fait qu'elle n'examine pas et ne prenne pas pleinement en considération d'autres initiatives parallèles de la Commission et d'autres procédures législatives en cours, comme la réforme de la protection des données et la proposition de règlement sur l'identification électronique et les services de confiance, la stratégie de cybersécurité n'offre pas de vision véritablement complète et globale de la cybersécurité au sein de l'Union et risque de perpétuer une approche fragmentée et compartimentée. Le CEPD note également que la directive proposée sur la sécurité des réseaux et de l'information ne permet pas encore une approche globale de la sécurité au sein de l'Union et que l'obligation prévue dans la législation sur la protection des données est probablement l'obligation de sécurité des réseaux et de l'information la plus complète dans le droit de l'UE.

78. Le CEPD déplore également que le rôle majeur joué par les autorités chargées de la protection des données dans la mise en œuvre et l'exécution des obligations de sécurité ainsi que dans le renforcement de la cybersécurité ne soit pas non plus dûment pris en considération.

79. En ce qui concerne la stratégie de cybersécurité, le CEPD met en lumière les éléments suivants:

- une définition claire des termes «cyber-résilience», «cybercriminalité» et «cyberdéfense» revêt une importance toute particulière dès lors que ces termes sont utilisés comme justifications pour certaines mesures spéciales susceptibles de porter atteinte aux droits fondamentaux, notamment les droits au respect de la vie privée et à la protection des données. Néanmoins, les définitions de la «cybercriminalité» fournies dans la stratégie et dans la convention sur la cybercriminalité restent très vagues. Il serait judicieux de disposer d'une définition claire et *restrictive* de la «cybercriminalité» plutôt que d'une définition trop étendue;

- la législation sur la protection des données devrait s'appliquer à toutes les actions de la stratégie, dès lors qu'elles concernent des mesures comprenant le traitement de données à caractère personnel. Bien que la législation en matière de protection des données ne soit pas spécifiquement mentionnée dans les sections portant sur la cybercriminalité et la cyberdéfense, le CEPD souligne que bon nombre des actions prévues dans ces domaines sont susceptibles d'impliquer le traitement de données à caractère personnel et, partant, de relever du champ d'application de la législation applicable en matière de protection des données. Il constate également que de nombreuses actions consistent en la mise en place de mécanismes de coopération, lesquels exigeront la mise en œuvre de garanties adéquates de protection des données en ce qui concerne les modalités d'échange de données à caractère personnel;

- les autorités chargées de la protection des données (APD) jouent un rôle majeur dans le contexte de la cybersécurité. En tant que gardiennes des droits des personnes en matière de respect de la vie privée et de protection des données, les APD sont activement engagées dans la protection de leurs données à caractère personnel, que ce soit hors ligne ou en ligne. En tant qu'organes de surveillance, elles devraient dès lors être suffisamment associées à la mise en œuvre de mesures ayant trait au traitement de données à caractère personnel (comme le lancement du projet pilote de l'UE consacré à la lutte contre les réseaux zombies et les logiciels malveillants). D'autres acteurs dans le domaine de la cybersécurité devraient également coopérer avec elles dans la réalisation de leurs tâches, par exemple dans l'échange de meilleures pratiques et dans les actions de sensibilisation. Le CEPD et les APD nationales devraient également participer de manière adéquate à la conférence de haut niveau qui se tiendra en 2014 pour évaluer les progrès accomplis dans la mise en œuvre de la stratégie.

80. En ce qui concerne la directive proposée sur la sécurité des réseaux et de l'information, le CEPD conseille aux législateurs:

- d'introduire plus de clarté et de sécurité à l'article 3, paragraphe 8, sur la définition des acteurs du marchés couverts par le champ d'application de la proposition et de dresser une liste exhaustive reprenant tous les acteurs concernés, afin de garantir une approche pleinement harmonisée et intégrée de la sécurité au sein de l'UE;

- de préciser à l'article 1er, paragraphe 2, point c), que la directive proposée s'applique aux institutions et organes de l'UE et d'ajouter une référence au règlement (CE) n° 45/2001 dans l'article 1er, paragraphe 5, de la proposition;

- de reconnaître un rôle plus horizontal pour cette proposition en ce qui concerne la sécurité, en prévoyant explicitement à l'article 1er qu'elle doit s'appliquer sans préjudice des règles plus détaillées, existantes ou futures, dans des domaines spécifiques (comme celles qui seront définies

concernant les fournisseurs de services de confiance dans la proposition de règlement sur l'identification électronique);

- d'ajouter un considérant pour expliquer la nécessité d'insérer la protection des données dès la conception et par défaut à un stade précoce de la conception des mécanismes établis dans la proposition et tout au long du cycle de vie des processus, procédures, organisations, techniques et infrastructures concernés, en tenant compte de la proposition de règlement sur la protection des données;

- de préciser les définitions de «réseau et système informatique» à l'article 3, paragraphe 1, et d'«incident» à l'article 3, paragraphe 4, et remplacer, à l'article 5, paragraphe 2, l'obligation d'élaborer un «plan d'évaluation des risques» par l'obligation d'«établir et maintenir un cadre de gestion des risques»;

- de préciser, à l'article 1er, paragraphe 6, que le traitement des données à caractère personnel serait justifié au titre de l'article 7, point e), de la directive 95/46/CE dans la mesure où il est nécessaire pour atteindre les objectifs d'intérêt public poursuivis par la directive proposée. Toutefois, il convient de veiller au respect des principes de nécessité et de proportionnalité afin que seules les données strictement nécessaires à la finalité à atteindre soient traitées;

- de définir à l'article 14 les circonstances dans lesquelles une notification est requise, ainsi que le contenu et le format de la notification, y compris les types de données à caractère personnel qui doivent être notifiées et si la notification et ses documents justificatifs incluront ou non des détails sur les données à caractère personnel (comme les adresses IP) affectées par un incident de sécurité spécifique et, le cas échéant, dans quelle mesure. Il convient de tenir compte du fait que les autorités compétentes en matière de SRI ne devraient être autorisées à collecter et à traiter des données à caractère personnel dans le cadre d'un incident de sécurité que si cette collecte et ce traitement s'avèrent strictement nécessaires. La proposition devrait aussi fournir des garanties suffisantes pour veiller à la protection adéquate des données traitées par les autorités compétentes en matière de SRI;

- de préciser à l'article 14 que les notifications d'incident visées à l'article 14, paragraphe 2, devraient s'appliquer sans préjudice des obligations de notification des violations de données à caractère personnel imposées par la législation applicable en matière de protection des données. La proposition devrait exposer les principaux aspects de la procédure relative à la coopération des autorités compétentes en matière de SRI avec les APD dans les cas où un incident de sécurité implique une violation des données à caractère personnel;

- de modifier l'article 14, paragraphe 8, afin que l'exclusion des micro-entreprises du champ d'application de la notification ne s'applique pas aux acteurs qui jouent un rôle crucial dans la fourniture de services de la

société de l'information, compte tenu notamment de la nature des informations qu'ils traitent (des données biométriques ou des données sensibles, par exemple);

- d'ajouter à la proposition des dispositions régissant l'échange ultérieur de données à caractère personnel par les autorités compétentes en matière de SRI avec d'autres destinataires, afin de garantir que: i) les données à caractère personnel ne soient divulguées qu'à des destinataires dont le traitement est nécessaire à l'accomplissement de leur mission conformément à une base juridique appropriée; et ii) ces informations sont limitées au strict nécessaire à l'accomplissement de leur mission. Il convient également d'examiner la manière dont les entités qui fournissent des données au réseau de partage d'informations garantissent le respect du principe de la limitation de la finalité;

- de définir le délai applicable à la conservation des données à caractère personnel conformément aux objectifs définis dans la directive proposée, notamment en ce qui concerne la conservation par les autorités compétentes en matière de SRI et au sein de l'infrastructure sécurisée du réseau de coopération;

- de rappeler aux autorités compétentes en matière de SRI leur obligation de fournir une information appropriée aux personnes concernées sur le traitement des données à caractère personnel, par exemple en publiant leur politique en matière de respect de la vie privée sur leur site web;

- d'ajouter une disposition relative au niveau de sécurité que les autorités compétentes en matière de SRI doivent respecter en ce qui concerne les informations collectées, traitées et échangées. Une référence aux exigences de sécurité visées à l'article 17 de la directive 95/46/CE devrait être spécifiquement introduite en ce qui concerne la protection des données à caractère personnel traitées par les autorités compétentes en matière de SRI;

- de préciser, à l'article 9, paragraphe 2, que des critères relatifs à la participation des États membres au système sécurisé d'échange d'informations devraient assurer qu'un niveau élevé de sécurité et de résilience soit garanti par tous les participants aux systèmes d'échange d'informations à toutes les étapes du traitement. Ces critères devraient inclure des mesures appropriées de confidentialité et de sécurité conformément aux articles 16 et 17 de la directive 95/46/CE et aux articles 21 et 22 du règlement (CE) n° 45/2001. La Commission devrait être expressément tenue de respecter ces critères pour participer en tant que responsable du traitement au système sécurisé de partage d'informations;

- d'ajouter à l'article 9 une description des rôles et responsabilités de la Commission et des États membres dans la création, l'exploitation et la maintenance du système sécurisé d'échange d'informations, et de prévoir que la conception du système devrait être conforme aux principes de

protection des données dès la conception et par défaut et de sécurité dès la conception; et

- de préciser à l'article 13 que tout transfert de données à caractère personnel vers des destinataires situés en dehors de l'UE doit être conforme aux articles 25 et 26 de la directive 95/46/CE et à l'article 9 du règlement (CE) n° 45/2001.

Fait à Bruxelles, le 14 juin 2013

(signé)

Peter HUSTINX
Contrôleur européen de la protection des données